Date 16/7/25

Ex:-1 Basic window & Linux Command

Aim:
To Study various network commands used in linux and windows.

Commands:

Windows:

i) arp -a (address resolution protocal) -
It will show ip address of the device, when it shows the IP address

O/P

172.16.10.107	d8-bb-C1-C5-6b-8C
172.16.10.108	d8-bb-C1-C5-Ce
172.16.10.11C	d8-bb-C1-C5-C0
172.16.10.114	d8-bb-C1-C5-C0
172.16.10.115	d8-bb-C1-C5-C0

2) hostname - It displays the name of your computer. O/P design - GOLVE J

3) IP Config - It display detailed configuration information. O/P hostname.: Desktop-GOLVE4J
Node type : hybrid
IP routing enable: NO

4) nbstat = Display protocol statistics and current TCP/IP connections using NBT

O/P:
> nbtstat - A 172.16.11.255

Ethernet:
Node Ip address: 172.16.10.1087.
scope ID: [ ]
host not found

5) netstat: Tool for monitoring network connections both incoming & outgoing

O/P:

> netstat -r

Kernel IP routing table

Destination	Gateway	Genmask	Flags
default	_gateway	0.0.0.0	UG
172.16.72.0	0.0.0.0	255.255.248.0	U

6) nslookup: It is a tool used to perform DNS lookups in linux. It is used to display DNS details, such as the IP address of a particular computer.

output: nslook www.google.com

Server: 127.0.0.53
Address: 127.0.0.53#53

Non-authoritative answer:
Name: www.google.com
Address: 142.250.195.196
Name:

7) Pathping: Pathping is a unique to window is and is basically a combination of the ping and tracert commands.

output:

Usage: pathping [-g host-list] [-h maximem-hops] [-n]

8) Ping: (Packet Internet Groper) command is the best ways to test connectivity between two nodes. Ping uses ICMP to communicate other devices.

Output:

>Ping google.com

PING google.com (142.251.221.206) 56(84) bytes of data.
64 bytes from Pnmaaa-ba-in-f14.1e100.net (142.251.221.206):

9) Route: route command is used to show/ manipulate the IP routing table. It is primarily used to setup static routes to specific host or networks via an interface.

Output:

Kernel IP routing table

Destination	Gateway	Genmask	Flag
Default	_gateway	0.0.0.0	UG
172.16.72.0	0.0.0.0	255.255.248.0	UG

Linux: Networking Commands:

i) IP: The ip command is one of the basic commands every administrator will need in daily work from setting up new systems and assigning IPs to troubleshooting existing systems.

Syntax:

ip <options> <object> <command>

a) ip address show

output:

1. lo: <loopback> mtu 65536 qdisc noqueue state unknown group default

2. enp0s31f6: <NO-CARRIER> mtu 1500 qdisc fq_codel state down group default

3. wlp2s0: <BROADCAST> mtu 1500 qdisc noqueue state UP group

b) IP address add 192.168.1.254/24 dev enp0s31f6:

output: connection established

c) ip lin

output:

enp0s
brd ff

d) ip
dev

output

dev
src

e) ip
192

outp
pro
net

f) ip

ou
en

2) if
n

c) ip link set enp0s31f6 up:

output:

enp0s31f6: link/ether 20:88:10:87:a2:ds
brd ffrff:ff:ff:ff:ff

d) ip route add default via 192.168.1.254
dev enp0s31f6

output: default via 192.168.1.254

dev enp0s31f6 proto kernel scope link
src 192.168.1.10

e) ip route delete 192.168.1.0/24 via
192.168.1.254

output: default via 172.16.72.0/21 dev
proto kernel scope link src 172.16.75.98
metric 60c

f) ip route get 10.10.1.24

output: 10.10.14 via 192.168.1.254 dev
enp0s31f6 src 192.168.1.10 cache

2) ifconfig: Configuring and trouble shooting
networks

output:

enp0s31f6: flag = 4099 <UP, BROADCAST,
MULLICAST7 mtu 150c

lo: flags = 73 <UP, LoopBACK, RUNNING> mtu 65536

wlp2s0: flags=4163 <UP, BROADCAST, RUNNING>
mtu 1500

3 mtr: Matt's traceroute serves as a network diagonstic and trouble shooting tool.

output:
mtr .google.com

	Host	Packets Loss%	Snt	Pings Last	Avg	Best	Wrst
1.	Gateway	1.2%	88	3.5	8.7	9.6	123.0
2.	172.16.12.122	0.0%	135	3.8	6.8	2.9	735.9

b) mtr -n google.com - Show numeric IP address (no. hostnames)

output:

1.	172.16.72.1	0.0%	82	2.4	3.6	1.8	39.9

c) mtr -b google.com - Show numeric IP & hostnames

output:

1.	(-gateway) 172.16.72.1	0.0%	282.9	43.2	2.2	

d) mtr -c 10 .google.com - Set number of (SNT) to be sent (pings)

output:

1.	-gateway	10.0%	10	45.4	8.0	2.4
	45.4	1.3				

4. ICpdum packets

a) Icpdum use.

Output:

all in

b) Icpdu on e

Outp

16:4

192

93.

c) Icp tru

Ou

16

16

16

4. Tcpdump: Designed for capturing and displaying packets

a) Tcpdumps -D - Show all interfaces tcpdump can use.

Output:
1. wlp2s0: [UP, Running, wireless]
2. any (Pseudo-device that captures on all interfaces)
3. Lo [Up, Running, Loopback]

b) Tcpdump -i eth0: It helps to capture the traffic on eth0:

Output:

16:42:00.123456

IP	Flag	Seq	Win
192.168.1.10.60432	S	123456789	29200
93.184.216.34.80	S	987654321	28960

c) Tcpdump -i eth0 -c 10: It helps to filter out traffic coming from a specific host.

Output:

IP	Flag	Seq	Length
16:42:00.123456	S	123456789	0
16:42:00.123789	S.	987654321	0
16:42:03.345678	P.	1:45	44

d) Tcpdump -i eth0 -c 10 host 8.8.8.8: It helps to filter out traffic coming from a specific host and to find traffic coming and going to 8.8.8.8

output:

IP	UDP	length
192.168.1.10.53321	8.8.8.8.53	32
192.168.1.10.53321	8.8.8.54	64
8.8.8.8.53	192.168.1.10.53322	48

e) Tcpdump -i eth0 src host 8.8.8.8: To filter traffic coming from 8.8.8.8

output:

IP	Flag	Seq	ack
16.44.00.12345 6	S.	98765	12345
16:44:02.234567	S.	556677	889900
16:44:03.345678	P.	100:140	50

f) Tcpdump -i eth0 dst host 8.8.8.8: To filter outbound traffic going to 8.8.8.8.

output:

IP	Flag	Seq	length
16:45:03.345678	P.	1:40	39
16:45:02.234567	S	234367	0

apsara

4) Tcpdump -i eth0 net 10.1.0.0 mask 255.255.255.0:

output:

16:42:21 - 123 89 IP 10.10.5.4431 > 10.1.0.12345

5) Tcpdump -i eth0 port not 53: and not 25: host 8.8.8.8: Captures specific host.

output:

16:48:00.123456 IP 192.168.1.10.60000 > 8.8.8.8.53: UDP, length 32

16:48:01.654321 IP 8.8.8.8.53 > 192.168.1.10.60000: UDP, length 64

6) Tcpdump -i eth0 port 53: Captures only DNS port 53

output:

16:47:00.123456 IP 192.168.1.10.50000 > 8.8.8.53: UDP, length 32

5) Ping: It is a tool that verifies IP-level connectivity to another TCP/IP Computer by sending internet Control message protocol (ICMP) echo request messages. and the recipt of corresponding echo reply messages is displayed.

Output:

ping google.com

PING google.com (216.58.206.174) 56(84) bytes of data

64 bytes from sof02s27-in-f14.1e100.net (216.58.

Page No.: 8

206.174): icmp_seq=1 ttl=56 time=10.7 ms

64 bytes from sof02s27-in f14.1e100: net C216.58.206
174): icmp_seq=2 ttl=56 time=10.2

Student Observation:

1) Which command is used to find the reachability of a host machine from your device?

Ans: Ping <host-name-or-IP-address>/Ping google.com

2) Which command will be give the details of hops taken by a packet to reach its destination?

Ans: ntr <hostname>
ntr & google.com

3) Which commands display the ip configuration of your machine?

Ans: Linux: IP address show, windows: ip config/all

4) Which command displays the TCP port states in your machine??

Ans: Netstat

5) Write the modify the ip configuration in a Linux machine?

Ans: to add: ip address add

to del: ip address del

Result:

The various network commands used in Linux and windows have been studied successfully.

21/7/25